AMENDMENT TO THE CLAIMS

1. (Currently Amended) A system comprising:

a first non-volatile data storage device, configured as one or more storage regions, to store one or more bytes of CMOS ~~BIOS~~ memory data, wherein the device lacks hardware security such that some of the CMOS ~~BIOS~~ memory data storage regions are modifiable by an application program on the system;

another, second non-volatile data storage device to store a mirror image of the CMOS ~~BIOS~~ memory data in a location that cannot be modified without system authorization;

a program store to store one or more processor-readable instructions to ascertain the validity of the CMOS ~~BIOS~~ memory data stored in the first non-volatile storage device and ~~if~~ when invalid to replace the CMOS ~~BIOS~~ memory data in the first non-volatile storage device with the stored mirror image of the data; and

a processing unit coupled to the first and second non-volatile data storage devices and program store, to read and process the one or more instructions in the program store.

2. (Previously Presented) The system of claim 1 wherein the processing unit is to process the instructions in the program store as part of a start-up procedure.

3. (Previously Presented) The system of claim 1 wherein the program store is inside said second non-volatile data storage device.

4. (Previously Presented) The system of claim 1 wherein the processor-readable instructions in the program store ascertain the validity of the data stored in the first non-volatile storage device on a region by region basis.

5. (Canceled).

6. (Previously Presented) The system of claim 4 wherein system authorization includes

employing a system interface to perform modifications to the data stored in said second non-volatile data storage device.

7. (Currently Amended) The system of claim 1 wherein ascertaining the validity of the CMOS ~~BIOS~~ memory data stored in the first non-volatile storage device includes

determining if ~~the~~ current data in the first non-volatile storage device is different than the stored image of the data.

8. (Currently Amended) The system of claim 1 wherein ascertaining the validity of the CMOS ~~BIOS~~ memory data stored in the first non-volatile storage device includes

determining if an integrity metric corresponding to ~~the~~ current data in the first non-volatile storage device is different than the same integrity metric corresponding to the stored image of the data.

9. (Currently Amended) The system of claim 1 further comprising:

generating a copy ~~the~~ of current data in the first non-volatile storage device ~~if~~ when an authorized application modifies the current data; and

storing the copy as a valid image of the current data.

10. (Currently Amended) A method comprising:

reading ~~current~~ CMOS ~~BIOS~~ memory content stored in a first non-volatile storage device of a system, wherein the first device lacks hardware security such that the CMOS ~~BIOS~~ memory content is modifiable by an application program in the system;

reading from a valid image of the CMOS ~~BIOS~~ memory content, that is stored in a further, second non-volatile storage device;

determining ~~if~~ when the ~~current~~ CMOS memory content in the first device has been modified without authorization; and

replacing the ~~stored current~~CMOS memory content with said stored valid image ~~of the content if~~when the ~~current~~ CMOS memory content is determined to have been modified without authorization.

11. (Currently Amended) The method of claim 10 wherein the determining comprises:

comparing the ~~read~~ valid image to the ~~current~~ CMOS memory content to determine ~~if~~ when the ~~current~~ CMOS memory content has been modified.

12. (Currently Amended) The method of claim 10 wherein determining ~~if~~ when the ~~current~~ CMOS memory content has been modified without authorization includes

comparing a previously stored checksum, corresponding to the valid image of the CMOS memory content, and a checksum corresponding to the ~~current~~ CMOS memory content.

13. (Currently Amended) The method of claim 10 wherein determining ~~if~~ when the ~~current~~ CMOS memory content has been modified without authorization includes

comparing a previously stored cyclic redundancy check value, corresponding to the valid image of the CMOS memory content, and a cyclic redundancy check value corresponding to the ~~current~~ CMOS memory content.

14. (Currently Amended) The method of claim 10 wherein determining ~~if~~ when the ~~current~~ CMOS memory content has been modified without authorization includes

comparing a previously stored bit mask, corresponding to the valid image of the CMOS memory content, and a bit mask corresponding to the ~~current~~ CMOS memory content.

15. (Currently Amended) The method of claim 10 further comprising:

storing a valid image of the ~~current~~ CMOS memory content for later use.

16. (Currently Amended) The method of claim 10 wherein reading the ~~current~~ CMOS memory content from the first non-volatile storage device is part of a start-up procedure of the system.

17. (Currently Amended) A method comprising:

arranging a first non-volatile storage device of a computer system into one or more storage regions to store CMOS ~~BIOS~~ data, wherein the device lacks hardware security such that some of the CMOS ~~BIOS~~ regions are modifiable by an application program in the system;

generating an integrity metric corresponding to valid CMOS ~~BIOS~~ content stored in a first region of the first non-volatile storage device; and

storing the integrity metric in another, second non-volatile storage device of the computer system to later determine ~~if~~ when the content in the first region has been modified without authorization.

18. (Currently Amended) The method of claim 17 further comprising:

comparing a previously stored integrity metric, corresponding to an earlier version of the content stored in the first region, to a newly calculated integrity metric corresponding to the current content stored in the first region to determine ~~if~~ when an unauthorized modification has occurred.

19. (Currently Amended) The method of claim 17 further comprising:

replacing the content of the first region with an earlier version of the content therein ~~if~~ when it is determined that there was an unauthorized modification.

Claims 20-30 (Canceled).